REMARKS/ARGUMENTS

Applicants amended claim 36 to correct the dependency and overcome the Examiner's objection on page 2 of the Office Action.

Applicants amended claims 6 and 30 to change the dependency to correct the antecedent basis and overcome the Examiner's indefiniteness rejection (35 U.S.C. §112, par. 2) on page 2 of the Office Action.

The Examiner rejected claims 1-4, 8-19, 21-30, and 34-40 as anticipated (35 U.S.C. §102) by Medveczky (U.S. Patent No. 5,182,77). Applicants traverse for the following reasons.

Amended independent claims 1, 16, and 27 concern distributing computer software from a first computer system, and require: receiving a request for software from a second computer system; generating a message; encrypting the generated message; transmitting the encrypted message to the second computer system; receiving an encrypted response from the second computer system; determining whether there is a code made available by the second computer system capable of decrypting the received encrypted response; decrypting the encrypted response with the determined code if there is one determined code; processing the decrypted response to determine whether the second computer system is authorized to access the software; and permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

Applicants amended claims 1, 16, and 27 to add the requirements of determining whether there is a code made available by the second computer system capable of decrypting the received encrypted response and decrypting the encrypted response with the determined code if there is one determined code, and that the decrypted response is processed to determine whether the second computer system is authorized to access the software.

Applicants submit that these added requirements to claims 1, 16, and 27 are not disclosed in the cited art. The Examiner cited col. 5, lines 46-52, col. 6, lines 46–49, and col. 5, lines 53-60 of Medveczky as disclosing the requirements of claims 1, 16, and 27. (Office Action, pg. 3).

The cited col. 5, lines 46-60 mentions that a subsystem may generate a password to authorize access to an application program, that is provided to a user that contacts the purveyor for access, and the purveyor uses this information to provide a password. The user would then

present this password to the user to access software. The cited col. 6 mentions that the generated password is suppled to the system user by known transmission routes.

Nowhere do the cited cols. 5 and 6 anywhere disclose the claim requirements of determining whether there is a code made available by the second computer system capable of decrypting the received encrypted response and decrypting the encrypted response with the determined code if there is one determined code, and that the decrypted response is processed to determine whether the second computer system is authorized to access the software. Instead, the cited cols. 5 and 6 discuss how the system may provide the user (second computer system) a code, but does not disclose determining whether the user has made a code available that is capable of decrypting a received encrypted response from the user as claimed.

The Examiner cited col. 7, lines 48-54 and col. 7, line 66 Medveczky to col. 8, line 2 as disclosing the claim requirements concerning encryption. (Office Action, pg. 3) Applicants submit that these cited sections do not disclose the claim encryption/decryption requirements.

The cited cols. 7-8 mention that the system performs encryption and/or decryption of specific information regarding the password and system identification codes, and that there are many encryption technologies, such as the use of a public key cryptography.

Although the cited cols. 7-8 discuss the use of encryption, nowhere do the cited cols. 7-8 anywhere disclose the claim requirement of determining whether there is a code made available by the second computer system capable of decrypting the received encrypted response and decrypting the encrypted response with the determined code if there is one determined code when determining whether to grant the second computer access to computer software.

Accordingly, claims 1, 16, and 27 are patentable over the cited art because the cited art does not disclose all the requirements of these claims.

Claims 2-4, 8-11, 17-19, 21-24, 28-30, and 34-40 are patentable over the cited art because they depend, directly or indirectly, from one of claims 1, 16, and 27. Moreover, certain of these claims provide additional grounds of patentability over the cited art for the reasons discussed below.

Amended claims 4, 19, and 30 depend from claims 1, 16, and 27, respectively, and further require that generating the message further comprises generating a random component to include within the message, and that determining whether the second computer system is authorized to

access the software further comprises determining whether the decrypted response includes the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the generated message.

Claims 4, 19, and 30 were amended to add the requirement that determining whether the second computer system is authorized to access the software further comprises determining whether the decrypted response includes the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the generated message.

The Examiner cited col. 8, lines 54-60 and col. 3, lines 18-22 of Medveczky as disclosing the requirements of claims 4, 19, and 30. (Office Action, pg. 3) Applicants traverse.

The cited col. 8 mentions that a random generator accepts a session key and that a second random number is accepted random number generator and assigned the value R. The cited col. 3 mentions a method for receiving an entered password, and comparing with a stored value corresponding to a machine configuration and software serial number to insure proper user authorization.

Applicants submit that the cited cols. 8 and 3 nowhere disclose that the random number is sent in a message to the user system (second computer), and then received back from the user computer in a encrypted response, that is decrypted, so that access is authorized if the decrypted response includes the generated message comprising the generated random number. Nowhere do the cited cols. 3 and 8 disclose this claimed use of the random number.

Further, the cited col. 8 uses the random number as part of a checksum, not a message transmitted back and forth between a first and second computer for use in determining whether the second computer has access to the software as claimed.

Accordingly, amended claims 4, 19, and 30 provide additional grounds of patentability over the cited art.

Claims 8, 21, and 34 depend from claims 1, 16, and 27, respectively, and further require that processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches

the generated message. The Examiner cited col. 8, lines 54-67 as disclosing the additional requirements of these claims. (Office Action, pg. 3) Applicants traverse.

The cited col. 8 discusses generating a random number for purposes of creating a checksum. Nowhere does the cited col. 8 anywhere disclose that determining whether the second computer can access the resource comprises determining whether the a message in the encrypted response matches a message the first computer sent to the second computer.

Accordingly, claims 8, 21, and 34 provide additional grounds of patentability over the cited art.

Amended claims 9, 11, 14, 22, 24, 26, 35, and 37 depend from base claims 1, 16, and 27, and additionally require that the message transmitted to the second computer system is encrypted with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system and that the encrypted response from the second computer system is encrypted with the second computer system's private key, wherein the first computer system has a public key of the second computer system for decrypting the encrypted response.

These claims also included the added requirement in the amendment that the code made available by the second computer system that is capable of decrypting the received encrypted response comprises the public key associated with the second computer system.

The Examiner cited the above discussed col. 7, line 66 to col. 8, line 2 as disclosing the additional requirements of these claims. (Office Action.). For the reasons discussed above, the cited cols. 7-8 nowhere disclose the claim requirement of determining whether there is a code made available by the second computer system capable of decrypting the received encrypted response, nor do these cited sections disclose that the code made available by the second computer system that is capable of decrypting the received encrypted response comprises a public key associated with the second computer system as claimed.

Accordingly, amended claims 9, 11, 14, 22, 24, 26, 35, and 37 provide additional grounds of patentability over the cited art.

Amended independent claims 12 and 25 concern accessing computer software from a first computer system with a second computer system and require: providing a code to the first computer system capable of decrypting an encrypted response from the from the second

computer system; transmitting a request for the software to the first computer system; receiving an encrypted message from the first computer system; processing the encrypted message to generate a response message; encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided code at the first computer system; transmitting the encrypted response message to the first computer system; and receiving access to the requested software in response to the encrypted response message.

Claims 12 and 25 were amended to add the requirements of providing a code to the first computer system capable of decrypting an encrypted response from the second computer system and encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided code.

The Examiner cited the same sections of Medveczky against claims 12 and 25 that were cited against independent claims 1, 16, and 27. Applicants submit that claims 12 and 25 distinguish over the cited Medveczky because they require providing a code to the first computer system capable of decrypting an encrypted response from the second computer system that includes a message from the first computer system, and encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided code at the first computer system.

For the reasons discussed above with respect to claims 1, 16, and 27, the cited Medveczky does not disclose the claim requirements of providing a code to the first computer system capable of decrypting a received encrypted response from the second computer system that includes a message the first computer system sent to the second computer system in an encrypted message to access the requested software that the second computer system, in turn, returns in the encrypted response to the first computer system to access the requested software.

Accordingly, claims 12 and 25 are patentable over the cited Medveczky because Medveczky does not disclose the claim requirements.

Claims 13-15 and 26 are patentable over the cited art because they depend from claims 12 and 25, respectively, which are patentable over the cited art for the reasons discussed above.

Claims 38-40 are patentable over the cited art because they depend, directly or indirectly, from claim 26, which is patentable over the cited art for the reasons discussed above.

The Examiner rejected claims 7, 20, and 33 as obvious (33 U.S.C. 103) over Medveczky in view of Hill (U.S. Patent No. 6,131,088). Applicants traverse this rejection on the grounds that claims 7, 20, and 33 depend from claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above.

The Examiner rejected claims 5, 6, 31, and 32 as obvious (33 U.S.C. 103) over Medveczky in view of Komura (U.S. Patent No. 5,994,307). Applicants traverse this rejection on the grounds that these claims depend from claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above. Moreover, these claims provide additional grounds of patentability over the cited art for the reasons discussed below.

First off, claims 5, 6, 31, and 32 are patentable over the cited art because they depend from claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above. Further, these claims provide additional grounds of distinction over the cited art for the following reasons.

Claims 5 and 31 depend from claims 1 and 27, respectively, and further require that the random component is comprised of a time stamp. The Examiner cited Komura as teaching the time stamp claim requirement. (Office Action, pgs. 4-5) Applicants traverse.

Although the cited Komura does discuss a timestamp, nowhere does the cited Medveczky or Komura, alone or in combination, anywhere teach or suggest that a message generated and encrypted and sent to a second computer system, which is then included in an encrypted response by the second computer system to the first computer system, comprises a timestamp.

Accordingly, claims 5 and 31 provide additional grounds of patentability over the cited art.

Claims 6 and 32 depend from claims 5 and 31 and further require that the time stamp is inserted at an offset into the message. These claims are patentable over the cited combination because they depend from claims 5 and 31, which are patentable over the cited art for the reasons discussed above, and because they. provide further requirements on the timestamp, which is not disclosed in the cited Medveczky.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-40 are patentable over the art of record. Applicants have not added any claims. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0466.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: October 2, 2003

By: _____

David W. Victor
Registration No. 39,867

Please direct all correspondences to:

David Victor
Konrad Raynes Victor & Mann, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984